OPPOSITION TO PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

Redacted Version of Document Sought to be Sealed

QUINN EMANUEL URQUHART & SULLIVAN, LLP

Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Sara Jenkins (CA Bar No. 230097)
sarajenkins@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

Andrew H. Schapiro (admitted *pro hac vice*)
andrewschapiro@quinnemanuel.com
Teuta Fani (admitted *pro hac vice*)
teutafani@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

Stephen A. Broome (CA Bar No. 314605)
stephenbroome@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
Crystal Nix-Hines (Bar No. 326971)
crystalnixhines@quinnemanuel.com
Alyssa G. Olson (CA Bar No. 305705)
alyolson@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

Josef Ansorge (admitted *pro hac vice*)
josefansorge@quinnemanuel.com
Xi (“Tracy”) Gao (CA Bar No. 326266)
tracygao@quinnemanuel.com
Carl Spilly (admitted *pro hac vice)*
carlspilly@quinnemanuel.com
1300 I Street NW, Suite 900
Washington D.C., 20005
Telephone: (202) 538-8000
Facsimile: (202) 538-8100

Jomaire Crawford (admitted *pro hac vice*)
jomairecrawford@quinnemanuel.com
51 Madison Avenue, 22nd Floor
New York, NY 10010
Telephone: (212) 849-7000
Facsimile: (212) 849-7100

Jonathan Tse (CA Bar No. 305468)
jonathantse@quinnemanuel.com
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Counsel for Defendant Google LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, OAKLAND DIVISION

CHASOM BROWN, *et.al*, individually and on behalf of all similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 4:20-cv-03664-YGR-SVK

GOOGLE LLC’S OPPOSITION TO PLAINTIFFS’ MOTION FOR CLASS CERTIFICATION

Judge: Hon. Yvonne Gonzalez Rogers
Date: September 20, 2022
Time: 2:00 p.m.
Location: Courtroom 1 – 4th Floor

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. BACKGROUND 3

A. Google's And Plaintiffs' Experts' Surveys Confirm That Class Members Had Divergent Knowledge And Expectations Regarding The Privacy PBM Provides 4

B. Forty Percent Of Named Plaintiffs And Numerous Other Putative Class Members Were Aware of Media And Academic Reports Discussing PBM Privacy Limitations 5

C. Class Members Can See In Real-Time That Google Receives The Data In PBM 6

D. The Inferences Plaintiffs Allege From Google's PBM Disclosures Were Not Shared By All Class Members 7

E. The Alleged Contract Is Not Uniform Over Time Or Across Classes 9

F. PBM Data Is "Orphaned" And Not Associated With Users' Identities Or With Their Browsing Activity In Other Modes 10

G. Google's Receipt And Use Of The Data Is Not Uniform Across The Class 11

III. ARGUMENT 12

A. Implied Consent Implicates Myriad Individual Issues—Including Standing—That Defeat Rule 23(b)(2)'s Predominance Requirement For All Claims 12

1. Numerous Sources Placed Users On Notice Of The Data Collection 13

2. Plaintiffs' Wiretap Act Claim Fails Predominance Twice Over Because Many Developers Were Also Aware of the Data Collection. 14

3. Plaintiffs Cannot Defeat Implied Consent Classwide 14

B. Plaintiffs' Seven Causes Of Action Require Further Individualized Inquiries 16

1. ECPA And CIPA § 631 Wiretapping Claims (Counts 1 And 2) 16

2. CIPA § 632 (Count 2) 17

3. CCCL/CDAFA Claim (Count 3) 17

4. Invasion Of Privacy (Count 4) And Intrusion Upon Seclusion (Count 5) 17

5. Breach Of Contract (Count 6) 20

6. UCL (Count 7) 21

C. Plaintiffs Fail To Show The Monetary Relief They Seek Is Available For All Class Members And To Proffer A Viable Classwide Damages Model 22

D. Certification Of An Injunctive Relief Class Should Be Denied 24

E. Plaintiffs Fail To Satisfy Rule 23(b)(3)'s Superiority Requirement 24

IV. CONCLUSION 25

TABLE OF AUTHORITIES

Page(s)

CASES

Am. Ex. Co. v. Italian Colors Rest.,
570 U.S. 228 (2013) 12

Backhaut v. Apple Inc.,
2015 WL 4776427 (N.D. Cal. Aug. 13, 2015) 12, 14, 15

Block v. eBay,
747 F.3d 1135 (9th Cir. 2014) 20, 21

Bowerman v. Field Asset Servs., Inc.,
2022 WL 2433971 (9th Cir. July 5, 2022) 22, 23

Byrd v. Aarons, Inc.,
2017 WL 4326106 (W.D. Pa. Aug. 4, 2017) 17

Calhoun v. Google,
526 F. Supp. 3d 605 (N.D. Cal. 2021) 12, 20

Campbell v. Facebook Inc.,
315 F.R.D. 250 (N.D. Cal. 2016) 12, 15

Capaci v. Sports Rsch. Corp.,
2022 WL 1133818 (C.D. Cal. Apr. 14, 2022) 24

Castillo v. Bank of Am., NA,
980 F.3d 723 (9th Cir. 2020) 22

Chowning v. Kohl's Dep't Stores, Inc.,
733 F. App'x 404 (9th Cir. 2018) 22

Comcast Corp. v. Behrend,
569 U.S. 27 (2013) 23

In re Facebook, Inc. Internet Tracking Litig.,
956 F.3d 589 (9th Cir. 2020) 18, 19, 20

Federated Univ. Police Officers' Ass'n v. Regents of Univ. of California,
2016 WL 9107427 (C.D. Cal. Aug. 18, 2016) 13, 18

Grosz v. Boeing Co.,
2003 WL 25669166 (C.D. Cal. Nov. 7, 2003), *aff'd*, 136 F. App'x 960 (9th Cir. 2005) 23

Harris v. comScore,
292 F.R.D. 579 (N.D. Ill. 2013) 14

Herskowitz v. Apple, Inc.,
301 F.R.D. 460 (N.D. Cal. 2014) 24

Hill v. Nat'l Collegiate Athletic Assn.,
7 Cal. 4th 1 (1994) 12

I.C. v. Zynga, Inc.,
2022 WL 2252636 (N.D. Cal. Apr. 29, 2022).....17, 18

In re Apple iPhone Antitrust Litig.,
2022 WL 1284104 (N.D. Cal. Mar. 29, 2022).....23

In re Facebook, Inc., Consumer Priv. User Profile Litig.,
402 F. Supp. 3d 767 (N.D. Cal. 2019) 21

In re Flash Memory Antitrust Litig.,
2010 WL 2332081 (N.D. Cal. June 9, 2010).....24

In re Google Assistant Priv. Litig.,
457 F. Supp. 3d 797 (N.D. Cal. 2020) 12, 19

In re Google Inc. St. View Elec. Commc'ns Litig.,
21 F.4th 1102 (9th Cir. 2021).....25

In re Google Inc., Gmail Litig.,
2014 WL 1102660 (N.D. Cal. Mar. 18, 2014).....1, 12, 14, 15, 16

In re Hulu Priv. Litig.,
2014 WL 2758598 (N.D. Cal. June 17, 2014).....25

In re Roundup Prod. Liab. Litig.,
385 F. Supp. 3d 1042 (N.D. Cal. 2019), *aff'd sub nom. Hardeman v. Monsanto Co.*,
997 F.3d 941 (9th Cir. 2021).....23

In re Zynga Privacy Litig.,
750 F.3d 1098 (9th Cir. 2014).....16

Moreno v. San Francisco Bay Area Rapid Transit Dist.,
2017 WL 6387764 (N.D. Cal. Dec. 14, 2017).....19

Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC,
31 F.4th 651 (9th Cir. 2022) 12, 22, 23

Opperman v. Path, Inc.,
2016 WL 3844326 (N.D. Cal. July 15, 2016) 23

Opperman v. Path, Inc.,
87 F. Supp. 3d 1018 (N.D. Cal. 2014) 17

Pemberton v. Nationstar Mortg. LLC,
331 F. Supp. 3d 1018 (S.D. Cal. 2018).....21

Rhynes v. Stryker Corp.,
2011 WL 2149095 (N.D.Cal. May 31, 2011).....22

Rodriguez v. Google LLC,
2021 WL 2026726 (N.D. Cal. May 21, 2021)..... 14, 17, 20

Shaw v. Regents of Univ. of Cal.,
58 Cal. App. 4th 44 (1997) 20

Sonner v. Premier Nutrition Corp.,
971 F. 3d 834 (9th Cir. 2020)....................21

Sussman v. ABC, Inc.,
186 F.3d 1200 (9th Cir. 1999)....................16

Torres v. Nutrisystem, Inc.,
289 F.R.D. 587 (C.D. Cal. 2013)....................13

TransUnion LLC v. Ramirez,
141 S. Ct. 2190 (2021) 12, 18

Wal-Mart Stores, Inc. v. Dukes,
564 U.S. 338 (2011) 2, 14, 21

Williams v. Apple, Inc.,
2020 WL 6743911 (N.D. Cal. Nov. 17, 2020) 22

Williams v. Apple, Inc.,
338 F.R.D. 629 (N.D. Cal. 2021) 15

Yoon v. Lululemon USA, Inc.,
549 F. Supp. 3d 1073 (C.D. Cal. 2021)....................16

STATUTES

18 U.S.C. § 2511 ....12, 16

Cal. Civ. Code § 3358....................24

Cal. Civ. Code § 3515....................12

Cal. Penal Code § 502(c) 12

Cal. Penal Code § 631 16

Cal. Penal Code § 632(a) 17

Fed. R. Civ. P. 23 .... 1, 12, 22, 24

OTHER AUTHORITIES

2 Newberg on Class Actions § 4:72 (5th ed.))....................25

I. INTRODUCTION

Plaintiffs ask the Court to certify a class of "tens of millions" on the purported basis that Google uniformly deceived the class into believing that private browsing mode ("PBM") would prevent Google from receiving data used to deliver ads and analytics services to the websites they visit. The undisputed record, however, establishes that individualized issues pervade Plaintiffs' claims, defeating Rule 23(b)(3)'s predominance prerequisite and requiring certification be denied.

For example, "[c]onsent is a defense to Plaintiffs' claims" and "can be … implied." Dkt. 113 (MTD Order) at 14. But "[i]mplied consent is an intensely factual question that requires," *inter alia*, "determining to what disclosures each Class member was privy and [] whether that specific combination of disclosures was sufficient to imply consent … lead[ing] to numerous individual inquiries that will overwhelm any common questions." *In re Google Inc., Gmail Litig.*, 2014 WL 1102660, at *16-18 (N.D. Cal. Mar. 18, 2014). Here, the "full panoply of disclosures" (*id.*) includes Google's many conspicuous disclosures that explained that while Chrome's PBM (Incognito) provides privacy "from other people who use your device," "websites, including the ads and resources on those sites" may "still see your activity" and thus Incognito does not "make you invisible on the internet." *Infra* § II.D. It also includes the dozens of news and academic reports published throughout the class period that make explicitly clear that PBMs do not provide complete privacy from entities online. Indeed, in 2015, Plaintiffs' expert, Bruce Schneier, wrote: "Remember that the private browsing option on your browser *only deletes data locally*. So while it's useful for hiding your [] viewing habits from your spouse, *it doesn't block internet tracking*." Ex. 33, at 153.[1] A *Wired* article he cites recounts "*the long-known fact* that Incognito isn't truly anonymous" because "Google [is] still tracking you in privacy mode." Ex. 108, at 2. There is even an easy-to-use feature in Chrome—used by one Plaintiff—that *shows* users PBM transmissions to Google in real-time.

In light of the abundant public disclosures and information explaining the nature and extent of the privacy PBM provides, it is not surprising that *both* parties' survey experts confirmed that, while some class members may indeed have been confused, a substantial number of class members

[1] "Ex. __" refers to the exhibits attached to the concurrently filed Broome Declaration.

were well aware of the data collection in PBM and believed they consented to it. *See infra* § II.A.

Google is entitled to argue at trial that the particular combination of information a given class member reviewed placed her on notice of the challenged conduct. The jury would then decide whether she impliedly consented. Because that individualized inquiry cannot be conducted in a class proceeding, implied consent defeats predominance and precludes certification of any claims. *See Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 367 (2011) ("[A] class cannot be certified on the premise that [defendant] will not be entitled to litigate [its] defenses to individual claims.").

Plaintiffs attempt to gloss over this problem by repeatedly mischaracterizing internal Google documents discussing potential user misconceptions about Incognito and suggesting that tens of millions of class members somehow *uniformly* misinterpreted Google's PBM disclosures. Most of the documents are unrelated to the specific data collection implicated by Plaintiffs' claims.[2] And if some users *were* confused about the privacy PBM provides, the studies Plaintiffs cite—and the parties' experts' surveys—show many others were not. That is precisely the point.

In addition to implied consent, class certification should be denied on other grounds:

First, Plaintiffs' seven disparate causes of action implicate standing issues and elements that cannot be proven class-wide, further defeating predominance.

Second, Plaintiffs fail to show that determinations of whether some class members were injured at all and individual damage calculations will not predominate, and their damages models are speculative and arbitrary.

Third, an injunctive relief class cannot be certified because the relief sought is only incidental to the damages claim and would affect many non-class members.

Finally, a class action is not superior because neither class members nor the data associated with their PBM sessions can be readily identified. By design, PBM data is not linked to Google Accounts but to cookie values automatically deleted from the browser at the end of each session.

[2] Namely, Google Account holders visiting non-Google websites in PBM while signed-*out* of their Accounts. *See, e.g.*, Pl. Ex. 9, at -183, -187 ("Chrome *Sign in* Awareness Survey" that asks about user awareness of features while *logged in*, and about Google's receipt of data through "search autocomplete," a feature not at issue here (emphasis added)).

The process of searching for Plaintiffs' *own* data confirms that their "fingerprinting" proposal—requiring a data process Google forbids and Plaintiffs condemned until they realized *they* needed it—is not reliable and cannot feasibly be scaled classwide. Even if it could, Plaintiffs' own experts concede it would result in misidentification, privacy violations, and user safety risks.[3]

II. BACKGROUND

Plaintiffs' case is based on a claim that putative class members were deceived about Google's receipt of data reflecting users' interactions with websites ("Data")[4] that have installed Google services to serve ads and conduct analytics ("Services"). The process by which Google and other web-services receive Data is ubiquitous. Zervas Decl. Ex. 1 (Zervas Rep.) ¶¶ 38-39; *id.* Ex. 2 (Zervas Rebuttal) ¶¶ 58-63. Even Plaintiffs' counsel and experts use these Services. Exs. 46-50.

It is undisputed that Google's Privacy Policy discloses the Data collection and that each Plaintiff read the Privacy Policy they contend is part of their contract.[5] Even more, Plaintiffs admit (1) the Data collection is "common knowledge," TAC ¶ 163; (2) they were aware of it before they filed suit;[6] and (3) they consented to it for modes other than PBM.[7] Accordingly, this case hinges

[3] Plaintiffs attempt to evade page limits with a 22 page argumentative "Trial Plan" and an additional 11 pages in Appendices. Dkt. 608-4. The Trial Plan fails to resolve any of the issues raised below.

[4] Plaintiffs' core complaint is that Google learned what websites they visited in PBM. They have broken this information down to the potential component parts of the transmissions (*e.g.*, URLs, cookies, IP address) at ¶ 63 of the TAC. They acknowledge that certain categories of Data are not uniformly "available" (*e.g.*, geolocation, User-ID). *Id.*

[5] TAC ¶ 268; Ex. 25 (Byatt), at 23:2- 18, 29:5-20; Ex. 26 (Davis), at 48:19-49:6, 51:11-18, 93:13-21; Ex. 27 (Brown), at 30:19-31:1, 33:2-4; Ex. 28 (Castillo), at 24:18-25:20; Ex. 29 (Trujillo), at 36:2-12; Exs. 1-4, 9 (Plaintiffs' R&O's to RFA 1).

[6] Ex. 25 (Byatt), at 153:15-21 ("It's common knowledge … everyone knows that that's Google's business model."); Ex. 26 (Davis), at 69:10-14 (Google's collection of web browsing activity in non-private mode is "common knowledge"); *id.* at 70:23-71:2 ("I don't assume privacy in … normal Chrome sessions."); Ex. 28 (Castillo), at 70:12-14 ("It's clear to me that when I'm searching Google in regular mode, and not Incognito mode, that [Google] collect[s] this data."); *id.* at 100:3-25 ("I understand when I am not in Incognito mode that Google will intercept my communications … per the statements … in the Google Privacy Policy."); Ex. 29, (Trujillo) at 56:11-12 ("in regular mode … I am aware that information is being collected").

[7] Ex. 29 (Trujillo), at 62:12-14 ("I know that in regular mode I am consenting to Google Analytics collecting my information."); Ex. 27 (Brown), at 61:2-5 ("I understand that, hey, if I go do normal browsing … my data's being collected [by Google], and that's the deal we have."); *id.* at 158:8-11

on Plaintiffs' claim that class members uniformly believed using PBM would *prevent* Google from receiving the Data, and that use of PBM *negated* their consent. The record shows otherwise.

A. Google's And Plaintiffs' Experts' Surveys Confirm That Class Members Had Divergent Knowledge And Expectations Regarding The Privacy PBM Provides

There is wide variance in internet users' understanding of how internet technologies work. PBM is no different. Google's expert, Professor On Amir, surveyed PBM users and confirmed a significant percentage expect little or no confidentiality from entities online:

- Shown just the Incognito Screen, more Chrome users ([redacted] expect that companies providing analytics and advertising services to the websites they visit in PBM—like Google—*probably do* or *do* receive IP address, URLs of sites visited, and cookies versus those ([redacted] that expect such companies *probably do not* or *do not* receive such information. Amir Decl. Ex. 1 (Amir Rep.) ¶ 56 & Tables 2 & 3 (similar results for other browsers).

- Shown the documents Plaintiffs claim comprise their contract (the Incognito Screen, the Privacy Policy, and the Chrome Privacy Notice), [redacted] of respondents expect Google receives their IP address in Incognito mode, while [redacted] expect that Google receives the URLs of sites visited and cookies. *Id.* ¶¶ 69, 73 & Tables 5 & 6.

- Modifying the Incognito Screen and the linked "Learn More" page to make explicitly clear that Google is among the entities that may see users' activity in PBM has no statistically significant impact on users' likelihood of using Incognito to research a sensitive topic. *Id.* ¶ 83 & Table 10.

Even the result-oriented rebuttal survey by Plaintiffs' expert, Mark Keegan,[8] who showed respondents only PBM splash screens,[9] confirms these variations:

- Only [redacted]—indicated a belief that they have *not* given consent to Google to collect and save their Internet browsing history" in PBM. Dkt. 608-10 (Keegan Rebuttal) ¶ 187.

("I think targeted advertising is a good thing. And [in] normal browsing mode … I've given consent. We have a deal. I get the deal.").

[8] Professor Amir details why Keegan's unorthodox "waterfall" methodology is deeply flawed, including because the number of "misinformed" respondents increases with every question and could easily be manipulated to show that 100% of users were misinformed, or that hardly any of them were. Amir Decl. Ex. 3 (Amir Supp. Rep.) at ¶ 3 & § IV.

[9] Inexplicably, Keegan did not test users' expectations after reading the documents Plaintiffs claim comprise the contract (*e.g.*, the Privacy Policy) or Google's other disclosures that explain PBM and Google's data collection practices. *See* Amir Decl. Ex. 3 (Amir Supp. Rep.), at §§ V, VI. Had he done so, his results and Professor Amir's would have aligned even more.

- [redacted] of all respondents agreed that "Google collects and saves my Internet browsing activity when I browse the Internet in private browsing mode," while [redacted] answered that "Google does not collect and save my Internet browsing activity when I browse the Internet in private browsing mode," *Id.* at Ex. 67.

- Of the [redacted] of respondents Keegan asked about consent, [redacted] indicated they consented to Google collecting and saving their browsing activity in PBM. Keegan did not ask *all* respondents about consent, but this result represents [redacted] of total respondents. *Id.* at Ex. 68.

- Roughly [redacted] of respondents who were asked whether they agreed that Google "collects and saves" "URL information," "IP address," "browsing activity," and "cookies" in PBM confirmed they did agree—[redacted] the number who disagreed. *Id.* at Ex. 72.

Google also periodically conducted surveys, which show that many users understood the purpose of Incognito mode: "[t]o get privacy from people who can see or share my devices" and "[m]y searches won't show up in my history." Ex. 44, at -327. Another survey showed that many users understood Incognito mode to "[p]revent activity or login information from being saved to my browser," or "...to my device." Ex. 45, at -558. In that survey, belief that Incognito mode provided privacy from Google ranked [redacted] *Id.* Third party studies have similar results. Ex. 153, at 2.

B. Forty Percent Of Named Plaintiffs And Numerous Other Putative Class Members Were Aware of Media And Academic Reports Discussing PBM Privacy Limitations

During the class period, the media and academics—*including Plaintiffs' own expert*—publicly discussed the fact that PBM does not prevent Google and other web-service providers from receiving the Data. Ex. 33, at 153 (Schneier writing in 2015 that PBM "*only deletes data locally*" and "*doesn't block internet tracking*"); Ex. 34, at 16 (Schneier writing in 2018 that "[s]ettings like Chrome's 'incognito mode' or Firefox's 'private browsing' keep the *browser* from saving your browsing history. It does not prevent any websites you visit from tracking you."). In 2019, *Wired* magazine acknowledged "*the long-known fact* that Incognito isn't truly anonymous" because "*Google [is] still tracking you in privacy mode, even on the most sensitive of sites*." Ex. 108. The article notes that "Google doesn't claim that incognito is a catch-all security salve":

> [PBMs] limit what's recorded on one machine—[they're] not an all-encompassing way to be private online.... In incognito mode, your data is tracked in exactly the same way as normal mode. The difference is that in ordinary circumstances, trackers are unable to link a 'private browsing' session with the 'normal session.'

Id. Dozens of similar articles were published in *USA Today*, *Consumer Reports*, *Cosmopolitan*, the

New York Times, the *NY Post*, *Huffington Post*, the *Washington Post*, *Computerworld*, and *PC Mag*, among others.[10] Given the breadth and diversity of the media outlets, many class members were aware of these reports. Indeed, two of five Plaintiffs admit they read such articles.[11]

C. Class Members Can *See* In Real-Time That Google Receives The Data In PBM

Easily available tools allow users to examine in real-time the information their browsers send in PBM and to whom; there is nothing "secret" about it. For example, Chrome has a user-friendly feature that displays the domains—including Google domains—receiving Data on the websites they visit, even in Incognito. Zervas Rep. ¶¶ 63 n.72, 65-67; McPhie Decl. § F. The feature is easy-to-use and other browsers have similar ones. Zervas Rebuttal ¶¶ 26, 121-124. While not all class members are familiar with these tools, many of them are. Indeed, Plaintiff Byatt testified that he was familiar with these tools, and they provide "a lot" of information, including the services the website uses and the domains (*e.g.*, Google.com) to which the Data is transmitted. Ex. 25 (Byatt), at 47:17-49:12. Plaintiffs even used Chrome's tool in drafting their complaint. *See* TAC ¶ 86.

There are other ways class members' understandings of what data Google receives in PBM will vary significantly. Users may click on the "Ad Choices" icon in the corner of any ad served by Google. McPhie Decl. ¶¶ 93-98. They may also be directly informed of Google's Data collection in PBM from the websites they visit (which naturally vary by user). *Id.* ¶ 80-92; Exs. 39, 51-104. Indeed, some websites have pop-ups (in PBM) that explain that the website is using Services that

[10] *See also e.g*., Ex. 110 (Incognito mode does not "protect you from Google search tracking or its trackers on other websites" and "while in Incognito mode, Google is still tracking your searches, and can use them to send intrusive ads at you across the Web on the millions of sites and apps that run Google ads"); Ex. 113 ("Just because you are using incognito mode, that doesn't mean … Google, Facebook, and Amazon can't track your activity."); Ex. 112 ("Google can still record the websites you browse while in Incognito Mode on the Chrome browser…."); Ex. 107 ("Private browsing is designed to avoid keeping traces of your browsing session *on your computer*" but "hides *none* of that [browsing] data [from] Big tech companies such as Facebook and Google….") (second emphasis in original); Ex. 109 ("private browsing mode clears your browsing history *only from your local machine* … not from anywhere else"); *see also* Exs. 105-156.

[11] Ex. 29 (Trujillo), at 27:21-28:12, 91:13-19, 117:24-118:8 (Trujillo's concerns about Google's collection of Data in PBM began "six or seven years ago" and she read an article prior to her involvement in this lawsuit stating that Google was "tracking information while I'm in incognito mode"); Ex. 26 (Davis), at 82:2-22 (Davis read articles stating that "things were not as they appear with regard to incognito" and Google was "aggregating information" in PBM).

send Data to Google. McPhie Decl. ¶ 92; Exs. 39, 98-104; Ex. 25 (Byatt), at 23:5-7, 29:5-31:10.

D. The Inferences Plaintiffs Allege From Google's PBM Disclosures Were Not Shared By All Class Members

Plaintiffs point to not a single disclosure stating that PBM prevents Google from receiving the Data. Instead, their claims hinge on inferences from Google's use of the words "private" and "control" to describe PBM in disclosures. Yet their own privacy expert admits PBM *does* provide "privacy" and "control," including vis-à-vis Google. Ex. 32 (Schneier), at 104:15-19, 139:1-7, 154:21-155:8. And Plaintiffs fail to show that class members either uniformly reviewed Google's disclosures—some of which were available only for parts of the class period—or that they were uniformly misled. Google's disclosures not only accurately described PBM but, as both parties' expert surveys demonstrate, did so in a manner many class members understood.

The Incognito Screen is a full-page notice shown to a user each time she enables Incognito in Chrome. It states: "Now you can browse privately, *and other people who use this device won't see your activity*." McPhie Decl. ¶¶ 68-71. It explains that, in Incognito, "Chrome [*i.e.*, the browser] won't save" information ordinarily stored locally—like browsing history and cookies. *Id.* The Incognito Screen also makes clear that the degree of privacy is limited because "[y]our activity may still be visible" to entities online. *Id*. Other browsers' splash screens do the same. McPhie Decl. § G. Plaintiffs' expert admits the "local privacy" aspect of PBMs is important to many users because they share devices. Ex. 32 (Schneier), at 134:5-135:16; Ex. 35 ("households are not units; devices are not personal; the purchaser of a product is not its only user"); Psounis Decl. Ex. 1 (Psounis Rep.) ¶ 163 n.218 (citing sources). Indeed, when asked why *he* did not use PBM, Schneier responded: "I never used a shared computer," Ex. 32 (Schneier), at 82:9-12, further confirming that many class members use PBM for local privacy, not privacy from Google.

The Incognito Screen makes clear that a user's activity is still visible to third parties, including websites, employers, and ISPs. McPhie Decl. ¶¶ 68-71. Plaintiffs' complaint is that it does not name "Google." That is unpersuasive. Providing a comprehensive list of entities to which a PBM user's activity might still be visible is not feasible. Ex. 41 (Fair), at 72:6-73:19. The disclosure that activity is still visible to others conveys to users that PBM privacy is limited.[12] And, importantly, survey evidence establishes that even changing the Incognito Screen to name "Google" has no statistically significant impact on users' likelihood of using Incognito. Amir Rep. § VIII.

In any event, the Incognito Screen includes a "Learn More" button that was clicked more than [redacted] times by U.S. users between August 1, 2016 and January 1, 2022. McPhie Decl. ¶ 73 & Ex. 17. For half the class period, the button linked to the "How private browsing works in Chrome" page in the Google Help Center explaining in more detail that "Incognito mode stops Chrome from saving your browsing history to your *local* history," but "[y]our activity … might still be visible to," among others: "websites you visit, *including the ads and resources used on those sites*"; "Search engines" and "web-service[s]." *Id.* ¶¶ 59, 73. This page was visited about [redacted] times between its launch in July 2017 and January 2022. *Id.* ¶ 59 & Ex. 17.

Beginning May 2020, the "Learn More" button linked to the "How Chrome Incognito keeps your browsing private" page, which similarly explains: "In Incognito, none of your browsing history, cookies and site data, or information entered in forms are saved *on your device*. This means your activity doesn't show up *in your Chrome browser history, so people who also use your device* won't see your activity." *Id.* ¶ 73-75. The page also explains "What Incognito mode doesn't do": "Prevent the websites you visit from serving ads based on your activity during an Incognito session." *Id.* This page was visited about [redacted] times between May 1, 2020 and January 2022. *Id.*

The Chrome Privacy Notice ("CPN") described Incognito mode as follows:

> You can limit the information *Chrome* stores *on your system* by using incognito mode or guest mode. In these modes, *Chrome* won't store certain information, such as: [] Basic browsing history information….
>
> **Cookies**. Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new cookies on your system while you are in these modes, but they'll only be stored and transmitted until you close the incognito or guest window.

Id. ¶ 55. Notably, Google defines "Chrome" and "Google" differently, and the CPN uses the terms differently. *See id.* ¶ 54 ("You can stop *Chrome* from accepting cookies *from Google* or other sites.

[12] Most websites are an amalgam of first *and third-party* code. Zervas Rep. ¶¶ 38-39; Ex. 36 (Hochman I), at 308:23-310:15 ("Website Provider" includes third party service providers). The Privacy Policy explains that Google is among these third-parties. McPhie Decl. ¶ 22.

Learn more."); *id.* ("*Chrome* periodically sends information *to Google* to check for updates … [etc.]"). Thus, the CPN's statement that Incognito limits what *Chrome* "stores on *your* system" cannot reasonably (or uniformly) be interpreted to mean it prevents *Google* from receiving the Data.

During the class period, the CPN linked to the Chrome Privacy Whitepaper which explains that Incognito "is a temporary browsing mode. It ensures that you don't leave browsing history and cookies *on your computer*. The browsing history and cookies are deleted only once you have closed the last incognito window. *Incognito mode cannot make you invisible on the internet*." *Id.* § D.2.

The Privacy Policy said nothing about Incognito or PBM until May 2018, when Google added a *single* reference in a paragraph about how users can "manage [their] privacy" "*in a variety of ways*" including "brows[ing] the web privately using Chrome in Incognito mode." *Id.* ¶¶ 27-28.

The "Search & browse privately" Help Center page is the only document Plaintiffs cite describing PBM generally—as opposed to Incognito specifically—and thus the only document potentially applicable to Class 2. This page was visited fewer than [redacted] times between its launch in 2016 and January 2022. *Id.* ¶ 76. Because the page describes browsers Google did not design and does not control, it does not make any "promises." Rather, it explains that "[p]rivate browsing works differently *depending on which browser you use*," and "*usually* means" that "[t]he searches you do or sites you visit won't be saved *to your device or browsing history*." *Id.* It makes clear that, in PBM, users still may see "search results and suggestions based on your location or *other searches you've done during your current browsing session*." *Id.* It also explains that if a PBM user signs-*in* to Google, "searches and browsing activity might be saved to your account."

Other PBM providers offer similar descriptions. For example, Firefox explains that its PBM "helps you obscure your online activity *from other people who use Firefox on your computer*, but does not make you invisible online." *Id.* ¶ 102. And Microsoft explains that "Websites can still personalize content for you during your InPrivate browsing session because cookies and other site permissions aren't deleted until you close all InPrivate windows." *Id.* ¶ 105.

E. The Alleged Contract Is Not Uniform Over Time Or Across Classes

Plaintiffs argue that "Google's form contract" is common evidence. Mot. 6. But the alleged contract changed materially through the class period. *See* Ex. 43 (alleged contract over time).

- The Terms of Service ("TOS") from the beginning of the class period to March 30, 2020 limit class members' damages for breach of contract to the amount they paid for the service, *i.e.*, $0. McPhie Decl. § A; Exs. 15-24, at Interrogatory No. 13 and RFA Nos. 26-28.
- Before March 30, 2020, the TOS expressly incorporated the Privacy Policy; from March 30, 2020 to January 5, 2022, the TOS was modified to say that the Privacy Policy was "not part of these terms"; on January 5, 2022, the latter language was removed. McPhie Decl. § A.
- The Privacy Policy did not mention Incognito mode until May 25, 2018, and did not mention PBMs other than Incognito until February 10, 2022. *Id.* ¶¶ 27 n.5 & 28.
- The "Search & browse privately" page Plaintiffs cite was only linked from the Privacy Policy beginning May 2018. *Id.* ¶¶ 24 n.4, 77-79.
- The Incognito Screen's "Learn More" button linked to three different Help Center articles during the class period, and in mid-2020 added a cookie blocker toggle that is on by default. *Id.* ¶¶ 72-73.

F. PBM Data Is "Orphaned" And Not Associated With Users' Identities Or With Their Browsing Activity In Other Modes

Google stores the Data using cookies associated with identifiers. Berntson Decl. ¶¶ 10-11; Psounis Rebuttal §§ III.A., C., & D. When a user enables Incognito, the browser automatically logs her out of her Google Account (and any other accounts), so that her activity is not saved in the Account. Berntson Decl. § B.2.; Zervas Rep. ¶¶ 72-73. In addition, a new "cookie jar" is created for the duration of the session so that previously existing cookies are not shared, making the user appear as a new user to websites and Google. Berntson Decl. § B.2; Zervas Rep. ¶¶ 63-65. Websites and their service providers (including Google) may deposit *new* cookies on the browser—so browsing may be tracked *during* an Incognito session—but these cookies are stored in the new cookie jar. Berntson Decl. § B.2. When the user ends the session by closing Incognito, cookies in the new jar are automatically deleted. *Id.*; Zervas Rep. ¶¶ 66-68. In Google's systems, the Data is keyed to a cookie value that no longer exists on the user's browser—it is "orphaned." Berntson Decl. ¶¶ 25-31, 43; Ex. 42 (McClelland), at 80:25-81:11, 82:4-15. The orphaned Data may reflect activity on only a single site or a handful of sites from that PBM session, depending on browsing habits. Ex. 32 (Schneier), at 140:13-15; Psounis Rep. ¶¶ 48-64; Ex. 26 (Davis), at 80:3-10. And (if they did not sign in, per the class definition), it is not tied to a user's Google Account. Berntson Decl. § B.2.

Plaintiffs and their experts spill much ink on various theories as to how Google *could* link

PBM activity with their Google Accounts by combining various identifiers like IP address and user-agent information—*i.e.*, "fingerprinting," a practice Google forbids. Berntson ¶¶ 4-5, 12, 42-43. It is undisputed, however, that (1) years of expansive discovery and voluminous expert reports have not turned up even a *single* instance in which Google identified a PBM user in this or any manner;[13] and (2) Plaintiffs' experts admitted they are merely hypothesizing as to what Google "*could* do," not opining on what it *does*. Ex. 32 (Schneier), at 112:15-20; Ex. 36 (Hochman I), at 234:9-13.

Locating Data associated with Plaintiffs' PBM sessions alone involved a complex months-long search process managed by a technical Special Master and requiring multiple iterations of trial-and-error searches. Ansorge Decl. ¶¶ 3-4. This labor-intensive and highly individualized process—necessitated by PBM's privacy-enhancing functionality (not deletion of Data by Google, as Plaintiffs argue)—shows the challenges in locating PBM Data. It could not be scaled to the class. Even if attempted, both parties' experts agree it would misidentify many class members and violate their privacy. Psounis Rebuttal ¶¶ 110-180 & Appendix E ¶ 42; Ex. 27 (Hochman II), at 473:24-476:4, 489:1-492:2; Ex. 22 (Schneier), at 129:23-131:23; 170:15-25; 188:24-191:19.

G. Google's Receipt And Use Of The Data Is Not Uniform Across The Class

Many factors impact whether a particular Google Service receives a given category of Data from a class member. For example, websites can prevent Google from collecting or using certain categories of Data by selecting certain features in Analytics and Ad Manager. Berntson Decl. § B.1; Ganem Decl. § B.1. Some PBMs, like Safari's, use an "IP blinding system" to obfuscate Data. Dkt. 608-12 (Hochman Rep.) ¶¶ 129-30, 163. PBM users can also enable an array of settings and tools to prevent Google from receiving or using Data. Berntson Decl. § B.2; Ganem Decl. §§ B.2-3; Zervas Rep. ¶¶ 119-147. These include cookie blockers, VPNs, browser extensions, ad blockers, and disabling Ads Personalization. *Id.* Several Plaintiffs used these tools. Ex. 26 (Davis), at 38:18-39:19 (VPN); Ex. 25 (Byatt), at 71:24-72:10 (ad blocker). Plaintiffs' expert admits these tools are widely used and he uses them. Ex. 33, at 40 (Chrome "has extensive controls to block or delete

[13] Plaintiffs' expert David Nelson's claim that Google can identify "private browsing data that … can be linked to specific individuals and devices" using merely an IP address is based on unconfirmed anecdotes and unsupported speculation. *See* Nelson Mot. to Exclude.

cookies, and *many people enable those features*"); Ex. 32 (Schneier), at 64:8-65:17.

III. ARGUMENT

Rule 23 "imposes stringent requirements for certification that in practice excludes most claims." *Am. Ex. Co. v. Italian Colors Rest.*, 570 U.S. 228, 234 (2013). Plaintiffs bear the burden to show by a preponderance of admissible evidence that they have met Rule 23's requirements. *Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC*, 31 F.4th 651, 664-65 (9th Cir. 2022).

A. Implied Consent Implicates Myriad Individual Issues—Including Standing—That Defeat Rule 23(b)(2)'s Predominance Requirement For All Claims

"He who consents to an act is not wronged by it." Cal. Civ. Code § 3515. Lack of consent is an element of certain claims asserted,[14] consent is defense to the others,[15] and it "can be … implied." *See* Dkt. 113 (MTD Order), at 14. Here, the record confirms that a substantial number of class members—at least a third even using Plaintiffs' flawed survey—impliedly consented to the Data collection, thereby defeating predominance. Indeed, because class members who consented have not been "wronged," Cal. Civ. Code § 3515, they lack Article III standing. *See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2209-12 (2021) ("Every class member must have Article III standing in order to recover individual damages.").

"Individual issues regarding [implied] consent are likely to overwhelmingly predominate" where, as here, "there is a panoply of sources from which [] users could have learned of Google's interceptions" including "Google disclosures, third-party disclosures, and news articles." *Gmail*, 2014 WL 1102660, at *17; *Campbell v. Facebook Inc.*, 315 F.R.D. 250, 266 (N.D. Cal. 2016) ("individual issues of implied consent do predominate … due to the media reports on the practice" because "as long as users heard about it from somewhere and continued to use the relevant features, that can be enough to establish implied consent"); *Backhaut v. Apple Inc.*, 2015 WL 4776427, at

[14] *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 828 (N.D. Cal. 2020) ("the plaintiff bringing a CIPA claim has the burden to prove that the defendant lacked consent"); 18 U.S.C. § 2511(2)(d) (consent exception); Cal. Penal Code § 502(c) ("without permission" is an element of CDAFA claim); *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 26 (1994) ("the plaintiff in an invasion of privacy case ... must not have manifested by his or her conduct a voluntary consent").

[15] *See Calhoun v. Google*, 526 F. Supp. 3d 605, 615 (N.D. Cal. 2021) ("Consent is [] a defense to Plaintiffs' breach of contract" and "UCL claim").

*14 (N.D. Cal. Aug. 13, 2015) (implied consent defeats predominance where "numerous sources of information … could have put some proposed class members … on notice of the [] interceptions."); *see also Torres v. Nutrisystem, Inc.*, 289 F.R.D. 587 (C.D. Cal. 2013) (implied consent defeats predominance); *Federated Univ. Police Officer's Ass'n v. Regents of Univ. of California*, 2016 WL 9107427, at *7 (C.D. Cal. Aug. 18, 2016) (same).

1. Numerous Sources Placed Users On Notice Of The Data Collection

Numerous diverse sources notified users that Google collects the Data in PBM. *First*, Plaintiffs admit the Privacy Policy, which they read and agreed to, disclosed that Google receives the Data. Although they contend certain disclosures (the Incognito Screen, Post-May 2018 Privacy Policy, and CPN) might give the *impression* Google would *not* collect the Data in PBM, *both* parties' survey experts confirmed that significant percentages of users understood from the disclosures that Google *does* receive the Data in PBM, and would continue to use PBM anyway. Amir Rep. §§ VI-VIII; Keegan Rebuttal ¶¶ 185-188 & Exs. 67-69, 71-73.

Second, Google Help Center pages explain what Incognito does and does not do. *Supra* § II.D. For example, the page linked to the Incognito Screen for half the class period describes that Incognito does not conceal activity from "websites you visit, *including the ads and resources used on those sites*." Many users understand Google is among the "ads and resources used" on websites because (1) Google discloses it in the Privacy Policy and other disclosures, McPhie Decl. ¶ 22; and (2) many websites prominently disclose that they use Google Services, as contractually required. *Id.* ¶¶ 80-92; Exs. 51-104. Plaintiffs even admit *they* were aware Google collects the Data to serve ads and provides Services to non-Google sites. *See supra* at nn.6-7.

Third, class members can use tools that allow them to *see* in real-time that Google receives the Data on non-Google sites while in PBM. *Supra* § II.C.

Finally, the fact that PBM provides privacy from others who use the same device, but does not prevent Google and other web-service providers from receiving the Data, was widely discussed in the media before and throughout the class period. *Supra* § II.B. Thus, "[a] fact-finder, in determining whether Class members impliedly consented, would have to evaluate to which of the various sources each individual user had been exposed and whether each individual knew about and consented to the interception based on the[se] sources …. lead[ing] to numerous individualized inquiries that will overwhelm any common questions." *Gmail*, 2014 WL 1102660, at *18.

2. Plaintiffs' Wiretap Act Claim Fails Predominance Twice Over Because Many Developers Were Also Aware of the Data Collection.

These same disclosures and tools would also provide notice of the Data collection in PBM to website developers, a more sophisticated group.[16] Because "one-party consent is a defense under the Wiretap Act, the Court would have to individually determine whether either a proposed class member *or* [the website using Google's Service] 'knew about and consented to the interception' based on the sources to which he or she was exposed." *Backhaut*, 2015 WL 4776427, at *15; *Rodriguez v. Google LLC*, 2021 WL 2026726, at *6 (N.D. Cal. May 21, 2021) (Seeborg, C.J.) (dismissing wiretap claim because "interceptions occurred with the consent of app developers").

Plaintiffs' suggestion that consent was somehow vitiated because Google tells developers that it "will adhere to its own Privacy Policy," TAC ¶ 76, was soundly rejected by Chief Judge Seeborg in a similar case by Plaintiffs' counsel against Google. He reasoned that this "consent-upon-consent rationale" both lacks legal support and fails to "grapple with its plainly untenable real-world implications." *Rodriguez*, 2021 WL 2026726, at *5.

3. Plaintiffs Cannot Defeat Implied Consent Classwide

Plaintiffs do not dispute that determining individual implied consent precludes certification, but rather contend, without support, that the defense will not be available. Notably, Plaintiffs have not sought or obtained any ruling barring this defense, thus it *must* be considered viable in assessing certification. *See Wal-Mart*, 564 U.S. at 367 ("a class cannot be certified on the premise that [defendant] will not be entitled to litigate [its] defenses to individual claims"). In all events, Plaintiffs' *en masse* challenges to implied consent can be readily dispatched. *First*, they resurrect the rejected argument that implied consent "will be resolved based on Google's classwide form contract." Mot. 18 (citing *Harris v. comScore*, 292 F.R.D. 579, 585 (N.D. Ill. 2013)). Judge Koh

[16] Developers widely know that browsers are designed *not* to indicate to websites or their service providers when a user is in PBM. Zervas Rebuttal ¶¶ 48, 93. Google also discloses that "Chrome doesn't tell websites, including Google, when you're browsing privately in Incognito mode." McPhie Decl. ¶ 74. This tells developers that Google receives Data in *both* regular mode *and* PBM.

found this argument, and *Harris*, "unpersuasive" because "express and implied consent are analytically distinct" and "a finder of fact [is] allowed to consider a broader set of materials in answering the factual question whether users impliedly consented." *Gmail*, 2014 WL 1102660, at *19. Indeed, in *Gmail*, *Campbell,* and *Backhaut*, the defendants all had form contracts with users.

Second, Plaintiffs argue (at 19) that Google "waived any implied consent defense" by stating in the Privacy Policy that "[w]e will not reduce your rights under this Privacy Policy without your explicit consent." But a user's implied consent—*i.e.*, their choice to use a service while aware of the conduct—is neither an action by Google nor an instance of reducing the user's rights.

Third, Plaintiffs contend news reports and Help Center pages describing PBM's privacy limits are "common to the class." Mot. 19 (citing *Williams v. Apple, Inc.*, 338 F.R.D. 629, 639 (N.D. Cal. 2021)).[17] No evidence supports that assertion which contravenes common experience. It would also mean *all* class members must be deemed to have read *all* the dozens of reports and help pages explaining PBM's privacy limits and chose to use it anyway. The reality is that many class members did not read all (or any) of these articles. Only two of five Plaintiffs did. Plaintiffs cannot invoke a counter-factual expedient to avoid the inconvenient truth that dooms their motion: determining what class members understood and from which sources requires individualized examinations.[18]

Fourth, Plaintiffs fail to show the Wiretap Act's consent exception uniformly applies because Google allegedly "acted with a tortious purpose" such as to "build user profiles to personalize ads." Mot. 20. "The focus [of the consent exception] is not upon whether the interception

[17] Judge Koh did not rule differently in *Williams*, finding merely that "widespread public disclosures by Apple and numerous media platforms" were "common to the class" *for purposes of resolving a "contractual ambiguity"* in a form contract. 338 F.R.D. at 639. More relevant here, in *Gmail*, Judge Koh recognized that, *for purposes of implied consent*, individualized issues predominate where "there is a panoply of sources" disclosing the conduct. 2014 WL 1102660, at *16-17.

[18] Plaintiffs' contention (at 19) that implied consent fails because none of the disclosures or articles explain Google's 'is_Chrome_incognito detection bit" is meritless. "To find implied consent, a fact-finder need not determine [] users had specific knowledge of the particular devices that intercepted their [communications]," she "need only be convinced based on surrounding circumstances that [] users were notified." *Gmail*, 2014 WL 1102660, at *20. Plaintiffs' statements regarding "discovery sanctions" are also misplaced since the Court denied the majority of the relief Plaintiffs sought and specifically held that the reliability of "incognito detection bit" to identify Incognito traffic remains "in dispute." Dkt. 588 at ¶ 131; *see also* ¶¶ 44, 178.

itself violated another law; it is upon whether the purpose for interception—its intended use—was criminal or tortious." *Sussman v. ABC, Inc.*, 186 F.3d 1200 (9th Cir. 1999). Each act Plaintiffs describe demonstrates a legitimate *commercial* purpose, not a tortious one. *See Gmail*, 2014 WL 1102660, at *19 (crime/tort exception does not apply where primary motivation "has plainly not been to perpetuate torts on millions of internet users, but to make money"). And again, Plaintiffs improperly seek at certification a sweeping *substantive* ruling on a claim element over which fair fact disputes exist at this stage. For example, Plaintiffs fail to show Google builds "user profiles" with PBM data;[19] that Google may use PBM data to "personalize ads" during an open PBM session is widely known and not tortious; and the record confirms PBM data can only be used for "conversions" if users *sign-in* to their Google Accounts (excluding them from the class) or in circumstances that do not apply uniformly. Berntson Decl. § C; Zervas Rebuttal ¶¶ 106-08.

B. Plaintiffs' Seven Causes Of Action Require Further Individualized Inquiries

1. ECPA And CIPA § 631 Wiretapping Claims (Counts 1 And 2)

Whether Google intercepted the "contents" of communications—an essential element of their wiretapping claims, 18 U.S.C. § 2511; Cal. Penal Code § 631—also depends on individualized inquiries that defeat predominance. Plaintiffs allege Google intercepted "contents" in the form of "URL requests [and] webpage browsing histories." TAC ¶ 208. But the Ninth Circuit has held that URLs may *not* be content *unless* they contain "search terms" or other information the user typed out. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1108-09 (9th Cir. 2014) ("information disclosed in the referer headers at issue here [*e.g.*, URLs] is not the contents of a communication"); *see Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082-83 (C.D. Cal. 2021) ("CIPA § 631(a)[ii] protects only the internal, user-generated material of a message"). Thus, whether a Google Service receives URLs that would be considered "content" may depend on individualized factors including the

[19] Plaintiffs use the term "user profiles" loosely to serve whatever suits their purpose. As demonstrated above in § II.F, data received during PBM sessions is *not* linked to a user's regular or PBM sessions, or their Accounts, but to a cookie value deleted from the user's device once she closes the session. Berntson Decl. ¶ 5 & § B.2. The so-called "profile" might consist of just a single site, not linked to the individual. Ex. 32 (Schneier), at 140:13-15. That is not a "user profile." Psounis Rebuttal Rep. ¶¶ 78-85; Zervas Rep. ¶¶ 3-6, 80-83.

website, the Service, and the given class member's actions. *See* Zervas Rebuttal ¶¶ 50-52; *see also* *Byrd v. Aarons, Inc.*, 2017 WL 4326106, at *14-*15 (W.D. Pa. Aug. 4, 2017) (denying certification of wiretap claim in light of need to analyze each communications' "specific content").

2. CIPA § 632 (Count 2)

Plaintiffs fail to show Google uniformly intercepted "confidential" communications. Cal. Penal Code § 632(a). "California courts 'have developed a presumption that Internet communications do not reasonably give rise to that expectation' [of confidentiality]." *Rodriguez*, 2021 WL 2026726, at *7. To rebut it, Plaintiffs must show not only that they reasonably expected their browsing "would not be 'recorded' by Google," but "that *nobody* (including the [website] developers) would record the communications," which requires "unique, definite circumstances." *Id.* (emphasis added). Plaintiffs cannot rebut the presumption class-wide merely by invoking Google's use of the word "private" to describe PBM because the disclosures make clear PBM activity is *not private* from a host of entities on the web. *Supra* § II.D; Exs. 5-9, at RFA Nos. 12, 14 (Plaintiffs knew their PBM activity was visible to websites and others); *supra* § II.A (surveys confirm many class members are aware Google "collects and saves" PBM data).

3. CCCL/CDAFA Claim (Count 3)

Plaintiffs fail to show Google uniformly overcame "technical or code-based barriers." *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1054 (N.D. Cal. 2014); Dkt. 113, at 32 n.7. Although many class members and some Plaintiffs *did* use "technical or code based barriers"—*e.g.*, VPNs, cookie blockers, *see supra* § II.F—Plaintiffs fail to show Google "overcame" any such barriers, let alone for the whole class. Contrary to Plaintiffs' contention (at 11), PBM never served as a "technical or code-based barrier," and their subjective belief that it *should have* is insufficient.

4. Invasion Of Privacy (Count 4) And Intrusion Upon Seclusion (Count 5)

The privacy claims cannot be certified for three additional reasons. *First*, "[i]n a class action, at least one named plaintiff must have standing." *I.C. v. Zynga, Inc.*, 2022 WL 2252636, at *6 (N.D. Cal. Apr. 29, 2022) (Gonzalez Rogers, J.). Because Plaintiffs fail to show that any of the PBM Data was tied to their personal identities, they lack standing for privacy claims. Contrary to their allegation that Google built "cradle-to-grave" profiles that "associate" PBM Data "with the user's

'Google profile,'" TAC ¶¶ 54, 69, 91-112, discovery has forced Plaintiffs to admit that never occurred. Indeed, it would require overriding Google's policies and protocols prohibiting such linking. Berntson Decl. ¶¶ 4-5, 12, 42-43; Psounis Rebuttal ¶¶ 77-85; Schwartz Decl. Ex. 1 (Schwartz Rebuttal) ¶¶ 81-92. Instead, Plaintiffs' experts now claim Google *potentially could* link PBM Data to their Accounts, in violation of its policies. *See* Ex. 32 (Schneier), at 112:17-20 ("[M]y report is about what [Google] could do…I have not seen reports from Google that show whether they do or do not do these things"); Hochman Rep. ¶¶ 226-27, 236-37; Ex. 36 (Hochman I), at 117:1-118:16 (acknowledging Data is "stored separately" but claiming "it *can* be linked up"). The mere *possibility* that Google could violate its own policies and protocols to associate PBM Data with Plaintiffs' Accounts is not sufficient. *See TransUnion*, 141 S. Ct. at 2209-12 ("In a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm."); *I.C.*, 2022 WL 2252636, at *8 (no standing for privacy claims because the "pieces of information" revealed to third parties, on their own, were not "so private that their revelation would be highly offensive," and plaintiffs did not allege "that any of their actual first or last names were exposed … suggesting that their anonymity is preserved.").

Second, Plaintiffs fail to establish a reasonable expectation of privacy class-wide. The parties' survey results and the dozens of articles and disclosures on PBM demonstrate class members have differing expectations of the nature and extent of the privacy PBM provides. *See supra* §§ II.A-D; *see also Federated*, 2016 WL 9107427 at *7 ("one's awareness that his or her conversation is being recorded would almost certainly undermine any purported 'reasonable expectation of privacy'").[20] Moreover, unlike in *Facebook Internet Tracking Litig.*, on which Plaintiffs rely (Mot. 10-11), here there is no evidence that Google compiled "a comprehensive browsing history of an individual." 956 F.3d 589, 606 (9th Cir. 2020). Rather, Plaintiffs argue (at 20) that Google "build[s] user profiles and personalize[s] ads *during* private browsing sessions"—which might be limited to

[20] Plaintiffs' reliance (Mot. 10) on the Ninth Circuit's motion to dismiss decision in *Facebook Tracking* is misplaced. At that stage, the Court did not have the opportunity to assess the extent to which Facebook's practices were publicly discussed or otherwise visible, as they are here. Further, the Court relied on Facebook's "*affirmatively state[ment]* that logged-out user data would not be collected." 956 F.3d at 602 (emphasis added). There is no such affirmative statement here.

one website—and that Google *could* link this Data to their identities (even though it doesn't).

Third, Plaintiffs fail to establish the "highly offensive" element class-wide. What constitutes a highly offensive act "requires a holistic consideration of factors such as the likelihood of serious harm to the victim," and "the degree and setting of the intrusion." *Facebook Tracking*, 956 F.3d at 606. These individualized factors cannot be assessed for a diverse class that includes:

- The many class members who enabled cookie blockers in PBM to prevent tracking and personalized ads even *within* PBM sessions. *Supra* § II.G.
- The many class members, like Plaintiffs Byatt and Davis, who use VPNs, ad blockers, or other privacy tools that prevent IP addresses and other Data from being sent to Google. *Id*.
- The many class members who disabled Ads Personalization, such that Google did not use the Data to deliver personalized advertisements. *Id*.

See Google Assistant, 457 F. Supp. 3d at 831 ("relevant factors [for offensiveness] include … the degree to which the recordings are anonymized"); *Moreno v. San Francisco Bay Area Rapid Transit Dist.*, 2017 WL 6387764, at *8 (N.D. Cal. Dec. 14, 2017) (sharing "anonymous client id ... and location" is not "highly offensive").

Tellingly, *all five Plaintiffs* admit that they continue to use Chrome in Incognito despite being fully aware of both the Data collection and other browsers that (according to Plaintiffs' experts) provide greater privacy protections.[21] Nor have most Plaintiffs taken any other steps to prevent Google from receiving the Data.[22] Plaintiffs cannot credibly contend that Google's conduct is "highly offensive" when they knowingly and voluntarily have continued their same browsing behavior since filing suit two years ago.[23] The same holds true for their counsel and experts—who

[21] Ex. 29 (Trujillo), at 117:11-13; Ex. 26 (Davis), at 72:17-73:14, 82:23-11; Ex. 25 (Byatt), at 14:12-15:16; Ex. 27 (Brown), at 92:5-11; Ex. 28 (Castillo), at 143:23-24; *see also* Hochman Rep. ¶¶ 113-115 & n.31, 129-130, 161 n.56, 163; Ex. 32 (Schneier,) at 41:7-45:8, 181:6-12; Ex. 33, at 91; *see also* Ex. 145 (article describing browser options to "push back against online tracking").

[22] Ex. 27 (Brown) at 84:3-14; Ex. 29 (Trujillo), at 111:17-25; Ex. 28 (Castillo) at 21:6-22:12; Exs. 5-9, at RFAs 18-20.

[23] Nor can Plaintiffs credibly argue that using the Data for advertising is "highly offensive" given their admission that they find the ads "helpful and useful." Ex. 29 (Trujillo) at 112:13-113:22; Ex. 25 (Byatt) at 24:14-21 ("I enjoy getting [ads for] new products and services"); Ex. 26 (Davis) at 72:12-15 (acknowledging "utility" to "targeted advertising"); Amir Rebuttal Rep. at ¶ 78 ("[m]any consumers … prefer more relevant personal ads over non-personalized ads" and citing sources).

continue to use the Google Services at issue on their own websites. Exs. 45-50; Ex. 31 (Keegan), at 225:10-226:10 (admitting he will not stop using Google Analytics).

5. Breach Of Contract (Count 6)

Certification of the contract claim should also be denied for additional reasons. *First*, the alleged contract was not "uniform" throughout the class period. *Supra* § II.E and Ex. 43 (chart). Due to material changes to the alleged contract over time, and the fact that class members did not uniformly use PBM throughout the class period, class members are subject to varying defenses depending on *when* during the class period they used PBM. Ex. 43. For example, class members who used PBM before March 31, 2020 are subject to TOS's provision limiting Google's liability for breach to the amount paid to use the service—*i.e.*, nothing. *See* McPhie Decl. § A. Class members who used PBM before May 25, 2018, are subject to the additional argument that the Privacy Policy did not contain the alleged "promises" because it did not mention Incognito or PBM (nor did it link to the "Search & browse privately" page). *Id.* ¶¶ 18, 27-28, 77-79. And class members who used PBM after March 31, 2020 are subject to the argument that they have no contract claim because, on that date, Google amended the TOS to state that the Privacy Policy—and the documents Plaintiffs claim are incorporated therein[24]—is "not part of these terms." *Id.* § A; *Calhoun*, 526 F. Supp. 3d at 615 (March 31, 2020 TOS "explicitly excluded Google's Privacy Policy"). Plaintiffs cannot simply presume all class members used PBM *throughout* the class period; their own PBM usage rebuts that presumption. *Compare* Ex. 12 (Castillo only "recalls using [Incognito] in approximately 2016 and 2017"), *with* Ex. 10 (Brown used Incognito only in "the last two years").

[24] Respectfully, Judge Koh's finding that the Incognito Screen and "Search & browse privately" article are incorporated into the Privacy Policy (Dkt. 363, at 15-16) is against the weight of California and Ninth Circuit authority. Documents "incorporated by reference" in a contract must be "clear[ly] and unequivocal[ly]" incorporated with an "explicit" reference. *See Shaw v. Regents of Univ. of Cal.*, 58 Cal. App. 4th 44, 54 (1997); *Facebook Tracking*, 956 F.3d at 610 (rejecting incorporation of document that was not explicitly referenced); *Rodriguez*, 2021 WL 6621070, at *4 (Google's "Help Page is not incorporated by reference into the Privacy Policy"). Moreover, these are plainly informational pages that do not constitute binding promises. *Block v. eBay*, 747 F.3d 1135, 1138-39 (9th Cir. 2014) (pages providing a "description of how [the defendant's] system works" but lack "explicit promissory language" are not binding). Regardless, even under Judge's Koh's reasoning, the Incognito Screen and the "Search & browse privately" page are not part of a contract prior to May 25, 2018 because the Privacy Policy did not mention PBM.

Thus, whether a given class member is subject to contract defenses, *or even has a contract claim at all*, depends on temporal factors that do not apply classwide.[25] *Wal-Mart*, 564 U.S. at 367.

Second, Plaintiffs' effort to certify a class of Safari, Internet Explorer, and Edge users (Class 2) is cursory. Plaintiffs fail to identify *any* contractual documents where Google makes binding promises about PBM generally, as opposed to Incognito specifically. This makes sense given Google did not design and does not control non-Chrome browsers. The *only* document Plaintiffs cite that refers to PBM generally is the "Search & browse privately" page, which was not incorporated into the contract at any point, and certainly not before May 25, 2018. *Supra* at 20 and n.23. Even if it were, it uses language too equivocal to constitute a binding promise. McPhie Decl. ¶ 76 ("[p]rivate browsing works differently *depending on which browser you use*," but "*usually* means…"); *see also Block*, 747 F.3d at 1138-39 (informational pages are not binding contracts).

Finally, Plaintiffs fail to show a uniform breach. As shown above in § II.G, many settings and tools affect whether Google receives Data in PBM, and a fact-finder may determine that they provided the "privacy" and "control" Plaintiffs purportedly expected—*e.g.*, using Incognito *and* a VPN would prevent "fingerprinting" even if Google engaged in that practice (it doesn't). But determining whether a class member used a particular tool or combination of tools, and whether the alleged promise was or was not in fact breached, requires individualized inquiries.

6. UCL (Count 7)

Certification of the UCL claim should be denied for the additional reason that Plaintiffs expressly limited it to Google's allegedly "unfair" and "unlawful" violations of other laws that provide legal remedies, TAC ¶¶ 279-281, and the Ninth Circuit has held there can be no UCL claim unless Plaintiffs establish that they *lack* "an adequate remedy at law." *Sonner v. Premier Nutrition*

[25] While the CPN was generally consistent during the class period, Plaintiffs cannot certify a contract claim based on that document alone given that it describes Incognito only as a way to "limit the information Chrome stores *on your system*." McPhie Decl. ¶¶ 55-56. *See In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 801 (N.D. Cal. 2019) ("simple failure to disclose a practice doesn't constitute a breach of contract."). The CPN also defines "Chrome" differently from "Google," and uses the terms such that they cannot mean the same thing. *See* McPhie Decl. ¶ 54; *see also Pemberton v. Nationstar Mortg. LLC,* 331 F. Supp. 3d 1018, 1038 (S.D. Cal. 2018) ("defined contract term [must be treated] according to the definition in the contract").

Corp., 971 F. 3d 834, 844 (9th Cir. 2020); *Williams v. Apple, Inc.*, 2020 WL 6743911, at *10 (N.D. Cal. Nov. 17, 2020).[26] The UCL claim also cannot be certified because Plaintiffs "may not seek disgorgement as a remedy under the UCL," and, as explained in § III.F, they fail to proffer a viable damages model for restitution, the "only monetary remedy" available. Dkt. 363 (MTD Order), at 3.

C. Plaintiffs Fail To Show The Monetary Relief They Seek Is Available For All Class Members And To Proffer A Viable Classwide Damages Model

Certification of a class would be error for another, fundamental reason: Plaintiffs fail to show by a preponderance of evidence that determinations of whether class members were injured at all and individual damage calculations will not overwhelm questions common to the class. *Bowerman v. Field Asset Servs., Inc.*, 2022 WL 2433971, at *8 (9th Cir. July 5, 2022) (reversing certification where plaintiffs "cannot show that the whole class suffered damages traceable to the[] alleged [wrong]" and cannot "present[] a method of calculating damages that is not excessively difficult").[27] Plaintiffs' damages models also fails *Daubert* because they are arbitrary, unreliable, and speculative.

First, Plaintiffs' damages models admittedly fail to exclude uninjured class members. *See Bowerman*, 2022 WL 2433971, at *9 (reversing certification where fact of injury "would implicate highly individualized inquiries on whether that particular class member *ever* [suffered the alleged wrong]"); Ex. 38 (Lasinski), at 45:10-13 (Plaintiffs' damages expert admitting model does not exclude uninjured class members). Uninjured class members include not only users who consented, *see supra* at §§ II.G, III.A, but, for Plaintiffs' restitution theory, also users who value the personalized advertisements and customized content they receive more than the Data is worth and are legally unharmed.[28] *Chowning v. Kohl's Dep't Stores, Inc.*, 733 F. App'x 404, 406 (9th Cir.

[26] That their legal claims may ultimately fail is irrelevant. *Rhynes v. Stryker Corp.*, 2011 WL 2149095, at *4 (N.D.Cal. May 31, 2011) ("Plaintiffs' argument that they will have no adequate remedy at law if their other claims fail is unavailing. Where the claims pleaded by a plaintiff *may* entitle her to an adequate remedy at law, equitable relief is unavailable." (emphasis in original)).

[27] *See also Olean*, 31 F.4th at 668-69 (Rule 23(b)(3) requires "common questions predominate[] over … individualized questions about injury or entitlement to damages"); *Castillo v. Bank of Am., NA*, 980 F.3d 723, 733 (9th Cir. 2020) (affirming denial of certification where plaintiff "has not provided a common method" to exclude class members who "have no actual injury").

[28] Mr. Lasinski's restitution model is also nonsensical because it would value Data from *all* traffic at [redacted], which is more than Alphabet's operating profits from *all products and services sold*

2018) ("Restitution requires that the value of what the plaintiff received was less than what the plaintiff paid."); Strombom Decl. Ex. 1 (Strombom Rebuttal) ¶¶ 48-54.

Second, Plaintiffs fail to "establish that 'there is a method, common across the class, for arriving at individual damages'" which is essential "to survive the predominance inquiry." *In re Apple iPhone Antitrust Litig.*, 2022 WL 1284104, at *16 (N.D. Cal. Mar. 29, 2022) (Gonzalez Rogers, J.). Where, as here, individualized damages calculations are "excessively difficult," the case fails the Supreme Court's "simple command that the case be 'susceptible to awarding damages on a class-wide basis.'"[29] *Bowerman*, 2022 WL 2433971, at *9 (citing *Comcast Corp. v. Behrend*, 569 U.S. 27, 32 n.4). Tacitly conceding there is no method for compensating class members in accordance with their respective harm, Plaintiffs' expert proposes to give class members fixed amounts, regardless of whether the class member was injured and the wide variances in: (1) the amount of Data Google received from each class member; (3) the extent to which Google profited from each class member's Data (if at all); and (3) the value each class member places on their Data. *See* Ex. 38 (Lasinski), at 142:14-23, 144:7-12; Lasinski Mot. to Exclude. This is improper. *Opperman v. Path, Inc.*, 2016 WL 3844326, at *14-15 (N.D. Cal. July 15, 2016) (denying certification where class damages model would "overcompensate some class members, while undercompensating others").[30]

Finally, Plaintiffs' expert's damages methodologies are arbitrary, unreliable, and therefore

in the U.S. See Lasinski Mot. to Exclude. Even if "otherwise admissible under *Daubert*, [such expert evidence is] inadequate to satisfy the prerequisite of Rule 23." *Olean*, 31 F.4th at 666 n.9 (certification not appropriate where expert evidence "demonstrated nonsensical results").

[29] Plaintiffs' argument (at 17) that they need not propose a method of apportionment because the "interests affected are not the defendant's" is contrary to the recent rulings by this Court in *Apple Antitrust* and the Ninth Circuit in *Bowerman*. The cases Plaintiffs cite are inapposite.

[30] Plaintiffs also fail to show *punitive* damages would be "both reasonable and proportionate to the *amount of harm to the plaintiff and to the general damages recovered*." *In re Roundup Prod. Liab. Litig.*, 385 F. Supp. 3d 1042, 1047 (N.D. Cal. 2019), *aff'd sub nom. Hardeman v. Monsanto Co.*, 997 F.3d 941 (9th Cir. 2021) (emphasis added). Because the "amount of harm" here, if any, varies greatly for each putative class member, punitive damages are inappropriate. *See Grosz v. Boeing Co.*, 2003 WL 25669166 (C.D. Cal. Nov. 7, 2003), *aff'd*, 136 F. App'x 960 (9th Cir. 2005) (denying certification because "determining … punitive damages for the class would require an endless litany of fact-specific inquiries into the circumstances of each individual class member" and "defeat the efficiencies of proceeding by class action.").

fail *Daubert*. Lasinski Mot. to Exclude. The *restitution* theory is based on data their expert admitted is "qualitatively and quantitatively" different from the Data Google allegedly misappropriated. *See id*. Plaintiffs' *unjust enrichment* damages fail to account for Google's costs and to subtract the revenue not attributable to the alleged wrongful conduct. *Id*. And each of the four bases Mr. Lasinski cites for statutory damages inflate the award because they compensate for far more than the alleged harm. *Id*. Even more, Plaintiffs fail to articulate which remedy ties to which claim, even though many claims do not give rise to *any* of these remedies,[31] and certain remedies are barred by the TOS.

D. Certification Of An Injunctive Relief Class Should Be Denied

Rule 23(b)(2) "does not authorize class certification when each class member would be entitled to an individualized award of monetary damages." *Capaci v. Sports Rsch. Corp.*, 2022 WL 1133818, at *18 (C.D. Cal. Apr. 14, 2022). Plaintiffs' "primary intent in this litigation is to recover damages for past conduct." *In re Flash Memory Antitrust Litig.*, 2010 WL 2332081, at *7 (N.D. Cal. June 9, 2010); *Herskowitz v. Apple, Inc.*, 301 F.R.D. 460, 481 (N.D. Cal. 2014) (Rule 23(b)(2) (certification not appropriate unless monetary relief sought is only incidental to injunctive relief); Mot. 23. Even if injunctive relief were appropriate, what Plaintiffs seek is infeasible, goes far beyond the alleged harm, and would detrimentally affect internet users outside the class.[32]

E. Plaintiffs Fail To Satisfy Rule 23(b)(3)'s Superiority Requirement

A court's considerations of the superiority requirement should include "the difficulties likely to be encountered in the management of a class action." Fed. R. Civ. P. 23(b)(3)(A)-(D). Indeed,

[31] Restitution is unavailable for privacy, contract, or CIPA claims. *See* Lasinski Mot. to Exclude. Plaintiffs' claim that unjust enrichment is available for breach of contract is contrary to law. Cal. Civ. Code § 3358 (limiting contract damages to amount no "greater ... than [the plaintiff] could have gained by the full performance on both sides").

[32] Plaintiffs seek injunctive relief to "preclude Google from further collecting private browsing information." Mot. 24. To do so, Google would need to identify PBM users, contrary to (1) internet standards, Zervas Rep. ¶ 43; Psounis Rebuttal ¶¶ 69-74, and (2) Plaintiffs' experts' opinion that doing so violates privacy, Dkt. 608-7 (Schneier Rep.) ¶ 86; Ex. 32 (Schneier), at 129:23-130:5, 131:21-23, 170:15-25. Plaintiffs also fail to explain how Google could identify such traffic for non-Chrome browsers. Plaintiffs' request that Google "delete the private browsing information that it previously collected and is currently storing," and "remove any services that were developed or improved with the private browsing information," Mot. 24, is infeasible.

manageability is "by [] far the most critical concern." 2 Newberg on Class Actions § 4:72 (5th ed.) (citing cases). Here, the Data is keyed to a pseudonymous identifier set in a cookie that is unique to that PBM session and automatically deleted at the end of the session. *Supra* § II.F. By design, Google cannot readily identify class members or their data. *Id*. The record is replete with evidence that Google's systems and policies are designed to ensure signed-out PBM users are *not* identified. Berntson Decl. ¶¶ 4-5, 12, 42-43; Psounis Rebuttal ¶¶ 35-68; Schwartz Rebuttal ¶¶ 76-100. Because "self-identification would be pure speculation," and "forensic verification of claims would be prohibitively costly and time-consuming," "it [i]s not feasible to verify class members' claims." *In re Google Inc. St. View Elec. Commc'ns Litig.*, 21 F.4th 1102, 1115 (9th Cir. 2021). Nor should the Court credit Plaintiffs' hypocritical contention that Google should use fingerprinting techniques to "identify class members and/or verify [their] claims." Mot. 22. Fingerprinting is a practice Plaintiffs *condemn*, TAC ¶¶ 8, 100-04, and is prohibited at Google for the purpose of identifying users, Schwartz Rebuttal ¶¶ 87-90; Psounis Rebuttal ¶¶ 95-108. Fingerprinting would also be prohibitively costly and time-consuming. *See* Ansorge Decl. ¶¶ 2-12. And Plaintiffs' expert acknowledges it would invade the privacy of users who do not want to be identified, and place some PBM users at risk of abuse. Ex. 32 (Schneier), at 130:2-5, 170:15-25; Schneier Rep. ¶ 101; Ex. 35; Psounis Rebuttal ¶¶ 172 n.234, 176. These concerns are amplified because Plaintiffs' proposed methodology is inaccurate and unreliable. Psounis Rebuttal ¶¶ 109-127, 153-155, 162-177, Appendix E. Indeed, Plaintiffs' expert admits that IP addresses are "dynamic," and thus a current IP cannot reliably be used to fingerprint data from the class period.[33] Ex. 32 (Schneier), at 186:13-23; *see also* Ex. 40 (Weisbrot), at 74:15-75:8.

IV. CONCLUSION

Plaintiffs' Motion for Class Certification should be denied.

[33] Self-reporting through claims forms or affidavits is no solution because, by design, there is no efficient way to confirm claims and users have incentives to make false claims. *See In re Hulu Priv. Litig.*, 2014 WL 2758598, at *14-23 (N.D. Cal. June 17, 2014) (rejecting self-reporting where claims "are not amenable to ready verification" because asking "whether the user remained logged into Facebook, cleared cookies, or used ad-blocking software" is "prone to … subjective memory problems" and damages of $2,500 per class member would "create incentives for claimants.").

DATED: August 5, 2022

Respectfully submitted,

QUINN EMANUEL URQUHART &
SULLIVAN, LLP

By *\/s/ Andrew H. Schapiro*
Andrew H. Schapiro

Andrew H. Schapiro (admitted *pro hac vice*)
andrewschapiro@quinnemanuel.com
Teuta Fani (admitted *pro hac vice*)
teutafani@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

Stephen A. Broome (CA Bar No. 314605)
stephenbroome@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
Crystal Nix-Hines (Bar No. 326971)
crystalnixhines@quinnemanuel.com
Alyssa G. Olson (CA Bar No. 305705)
alyolson@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Sara Jenkins (CA Bar No. 230097)
sarajenkins@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

Jomaire A. Crawford (admitted *pro hac vice*)
jomairecrawford@quinnemanuel.com
51 Madison Avenue, 22nd Floor
New York, NY 10010
Telephone: (212) 849-7000
Facsimile: (212) 849-7100

Jomaire A. Crawford (admitted *pro hac vice*)
jomairecrawford@quinnemanuel.com
51 Madison Avenue, 22nd Floor
New York, NY 10010
Telephone: (212) 849-7000
Facsimile: (212) 849-7100

Josef Ansorge (admitted *pro hac vice*)
josefansorge@quinnemanuel.com
Xi ("Tracy") Gao (CA Bar No. 326266)
tracygao@quinnemanuel.com
Carl Spilly (admitted *pro hac vice*)
carlspilly@quinnemanuel.com
1300 I Street NW, Suite 900
Washington D.C., 20005
Telephone: (202) 538-8000
Facsimile: (202) 538-8100

Jonathan Tse (CA Bar No. 305468)
jonathantse@quinnemanuel.com
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Attorneys for Defendant Google LLC